

What is claimed is:

1. A method to monitor a network by a network monitor, comprising:

- 5 routing data packets through a router;
generating flow records for at least some of said data packets;
filtering said at least some of the flow records;
extracting packet information from the filtered flow records, wherein
the extracted packet information comprises internet information of at least one target
10 of interest; and
performing active measurements to said target of interest using the
extracted packet information.

2. The method according to claim 1, said filtering step
15 comprising:
selecting flow records based on an address field of said flow records.

3. The method according to claim 2, said filtering step comprising
selecting flow records having destination or source of non-local hosts.

- 20 4. The method according to claim 2, said filtering step comprising
selecting data packets having destination or source of local hosts.

5. The method according to claim 2, said filtering step comprising
25 selecting flow records containing critical services based on the address field or a port
field of the flow records.

6. The method according to claim 1, said filtering step comprising randomly selecting data packets from said filtered data packets.

5 7. The method according to claim 1, wherein said active measurements comprise a ping process.

8. The method according to claim 1, wherein said active measurements comprise a traceroute process.

10 9. The method according to claim 1, wherein said active measurements are selected based on said target of interest.

10. An apparatus for monitoring a network, comprising:
15 a router for routing data packets, wherein said router generates flow records for at least some of said data packets; and

a monitor for receiving the flow records, wherein said monitor filters said flow records, and further wherein said monitor extracts packet information from said filtered flow records, the extracted packet information comprising internet
20 information of at least one target of interest, wherein said monitor performs active measurements to said target of interest using the extracted packet information.

11. The apparatus according to claim 10, wherein said monitor filters said flow records based on an address field of each flow record.

25

12. The apparatus according to claim 11, wherein said monitor selects flow records having destination or source of non-local hosts.

13. The apparatus according to claim 11, wherein said monitor
5 selects flow records having destination or source of local hosts.

14. The apparatus according to claim 11, wherein said monitor selects data packets for critical services.

10 15. The apparatus according to claim 10, wherein said monitor randomly selects flow records from the flow records received by said monitor.

16. The apparatus according to claim 10, wherein said active
measurements comprise a ping process
15

17. The apparatus according to claim 10, wherein said active measurements comprise a traceroute process.

18. The apparatus according to claim 10, wherein said active
20 measurement are selected based on said target of interest.

19. A method to monitor a network by a network monitor,
comprising:

routing data packets through a router;
25 generating flow records for at least a fraction of said data packets;

extracting packet information from at least a fraction of said flow records, wherein the extracted packet information comprises internet information of at least one target of interest; and

performing active measurements to said target of interest using the
5 extracted packet information.

20. The method according to claim 19, said generating step comprising:

filtering said data packets; and
10 creating flows records for said filtered data packets.

21. The method according to claim 20, said extracting step comprising:

sampling said generated flow records; and
15 obtaining packet information from said sampled flow records.

22. The method according to claim 20, said filtering step comprising:

selecting flow records based on an address field of said flow records.
20

23. The method according to claim 20, said filtering step comprising selecting flow records having destination or source of non-local hosts.

24. The method according to claim 20, said filtering step
25 comprising selecting data packets having destination or source of local hosts.

25. The method according to claim 20, said filtering step comprising selecting flow records containing critical services based on the address field or a port field of the flow records.

5 26. The method according to claim 19, wherein said active measurements comprise a ping process

27. The method according to claim 19, wherein said active measurements comprise a traceroute process.

10